Tabla de contenido

1. OBJETIVOS 2
2. ALCANCE 2
3. GLOSARIO 3
4. DESARROLLO 3
   4.1. Cronograma de ejecución del Plan 3
   4.2. Seguimiento y Control del Plan 4

1. OBJETIVOS

OBJETIVO	ACTIVIDAD	META
Establecer los lineamientos, actividades y responsabilidades necesarios para gestionar de forma integral los riesgos de seguridad y privacidad de la información en la Dirección General Marítima (DIMAR), mediante la identificación, análisis, valoración, tratamiento y seguimiento de dichos riesgos, de acuerdo con los principios y metodologías del Modelo de Seguridad y Privacidad de la Información (MSPI). El propósito es reducir la exposición a amenazas, garantizar la continuidad operativa y fortalecer la protección de los activos de información institucionales.	Desarrollar el Cronograma de ejecución del plan para la vigencia 2026, establecido en la numeral 4.1	100%

2. ALCANCE

El presente documento responde a la necesidad de fortalecer la gestión integral de los riesgos asociados a la seguridad y privacidad de la información, considerando que la materialización de estos puede comprometer el cumplimiento eficiente, efectivo y óptimo de los objetivos institucionales de la Dirección General Marítima (DIMAR), tanto en su gestión interna como en la prestación de servicios a la ciudadanía.

En este contexto, la gestión de riesgos se consolida como una herramienta estratégica para el desarrollo, la implementación y la mejora continua de los procesos institucionales, al garantizar la protección del valor organizacional mediante la preservación de la confidencialidad, integridad y disponibilidad de la información, tanto en su forma física como digital.

Con base en esta premisa, la DIMAR formula el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026, atendiendo a las necesidades institucionales en materia de seguridad y asegurando el cumplimiento de las normativas aplicables, particularmente las establecidas en el Modelo de Seguridad y Privacidad de la Información (MSPI) y en las normas ISO/IEC 27001:2022 e ISO/IEC 27005:2022.

Este plan se enmarca en el ciclo de mejora continua PHVA (Planificar, Hacer, Verificar, Actuar) y se encuentra alineado con la Política de Seguridad de la Información de la Entidad, garantizando una gestión estructurada, medible y efectiva de los riesgos que puedan afectar la seguridad y privacidad de la información institucional.

3. GLOSARIO

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.

Consecuencia: Efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que modifica al riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Vulnerabilidad: Debilidad, atributo, causa o falta de control que permitiría a explotación por parte de una o más amenazas contra los activos.

MSPI: Modelo de Seguridad y Privacidad de la Información.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO. Es certificable. Primera publicación en 2005, segunda publicación en 2013, tercera publicación en 2022.

4. DESARROLLO

A continuación, se describen las actividades a realizar, tiempo de ejecución y responsables:

4.1. Cronograma de ejecución del Plan

N°	NOMBRE DE LA TAREA	FECHA INICIAL	FECHA FINAL	RESPONSABLE
1	Actualización del mapa de riesgos de seguridad de la información (P6 MSPI) y valoración de riesgos residuales	01/02/2026	30/04/2026	Oficial de Seguridad de la Información
2	Actualizar matriz DOFA - factores externos e internos que puedan afectar la seguridad digital y de la información de acuerdo con los cambios en el contexto de la entidad.	01/03/2026	15/05/2026	Oficial de Seguridad de la Información

N°	NOMBRE DE LA TAREA	FECHA INICIAL	FECHA FINAL	RESPONSABLE
3	Revisión y actualización de la metodología de análisis y tratamiento de riesgos según MSPI y ISO 27005.	01/03/2026	30/04/2026	Oficial de Seguridad de la Información
4	Definir las responsabilidades para la gestión del riesgo de Seguridad de la Información y la aceptación de los riesgos residuales.	01/07/2026	30/09/2026	Oficial de Seguridad de la Información
5	Definición e implementación de controles correctivos y preventivos (administrativos, técnicos y físicos).	16/05/2026	18/09/2026	Oficial de Seguridad de la Información
6	Identificar, valorar y analizar los riesgos del Subsistema de Seguridad de la Información y de Seguridad informática del proceso E3. Incluye la revisión y actualización del mapa de riesgos	01/07/2026	31/08/2026	Oficial de Seguridad de la Información
7	Realizar pruebas del plan Impacto al Negocio (BIA) para sistemas de información críticos (Fase 3).	01/08/2026	31/10/2026	Oficial de Seguridad de la Información
8	Elaborar análisis y reporte de eventos de incidentes de seguridad de la información.	01/10/2026	30/11/2026	Oficial de Seguridad de la Información
9	Ejecución de pruebas del DRP - Disaster Recovery plan - fase 3.	01/07/2026	30/09/2026	Oficial de Seguridad de la Información

4.2. Seguimiento y Control del Plan

El control de las actividades del plan será efectuado por el Oficial de Seguridad de la Información de la Dimar, por medio de la presentación de informes de gestión, las actividades se encuentran cargadas como tareas y responsabilidades del Oficial de Seguridad de la Información en la plataforma SIMEC, con las cuales se realizará seguimiento a la ejecución de estas.